

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-308835

(43)Date of publication of application : 17.11.1998

(51)Int.Cl.

H04N 1/00

G03G 21/04

H04N 1/21

(21)Application number : 10-053958

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 05.03.1998

(72)Inventor : KUWANO HIDEYUKI
MURATA KAZUYUKI
YAMAGUCHI TAKEHITO
OKADA YUJI
TAKAHASHI NAOKI
HISATOMI KENJI

(30)Priority

Priority number : 09 49991

Priority date : 05.03.1997

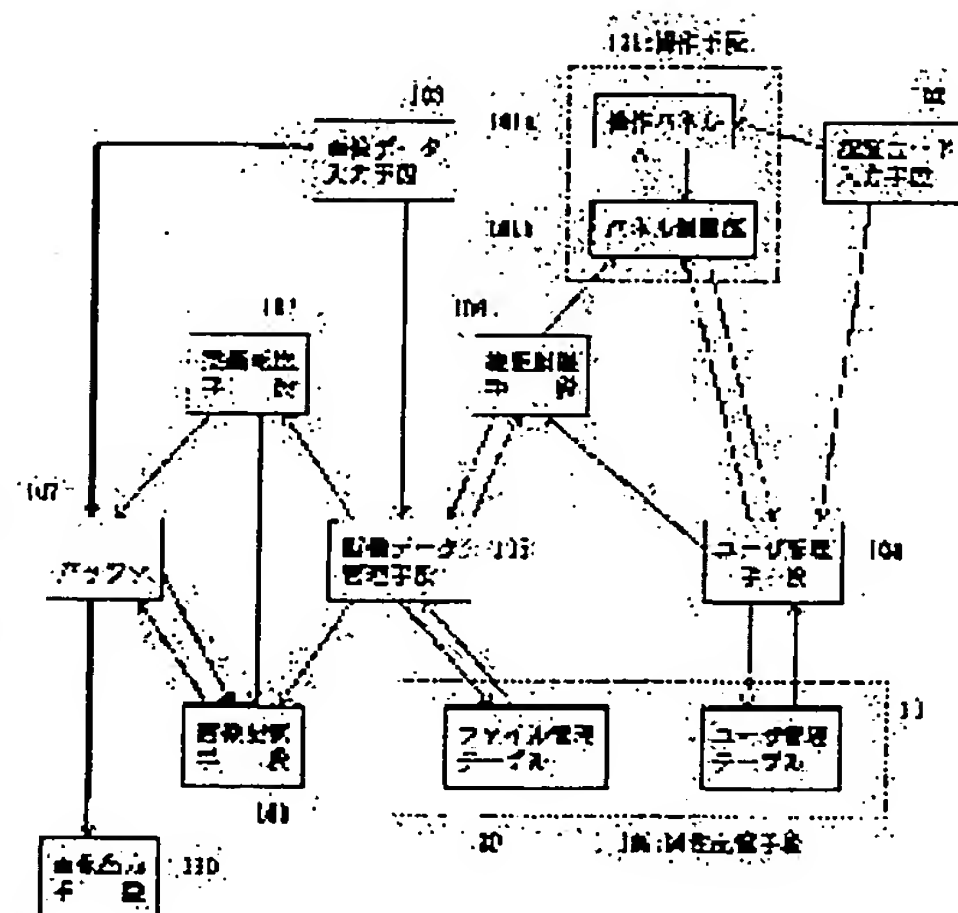
Priority country : JP

(54) IMAGE PROCESSING UNIT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the image processing unit that enhances confidentiality of recorded image data without making the operation complicated.

SOLUTION: The processing unit is provided with an authentication code input means 102 that reads an authentication code from an authentication medium on which a specific authentication code is stored, a user ID entry means that is used to enter user ID information including a specific user authentication number issued at user registration, a user management means 104 that manages the users based on the authentication code and the user ID information, and a function limit means 106 that limits a range of functions available for the user when the user cannot be specified based on the authentication code received from the authentication code input means 102 or the user ID information entered from the user ID entry means. Then storage of image data by an unspecified user is prevented and the confidentiality of stored image data is ensured.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

(43)公開日 平成10年(1998)11月17日

審査請求 未請求 請求項の数15 O.L (全 17 頁)

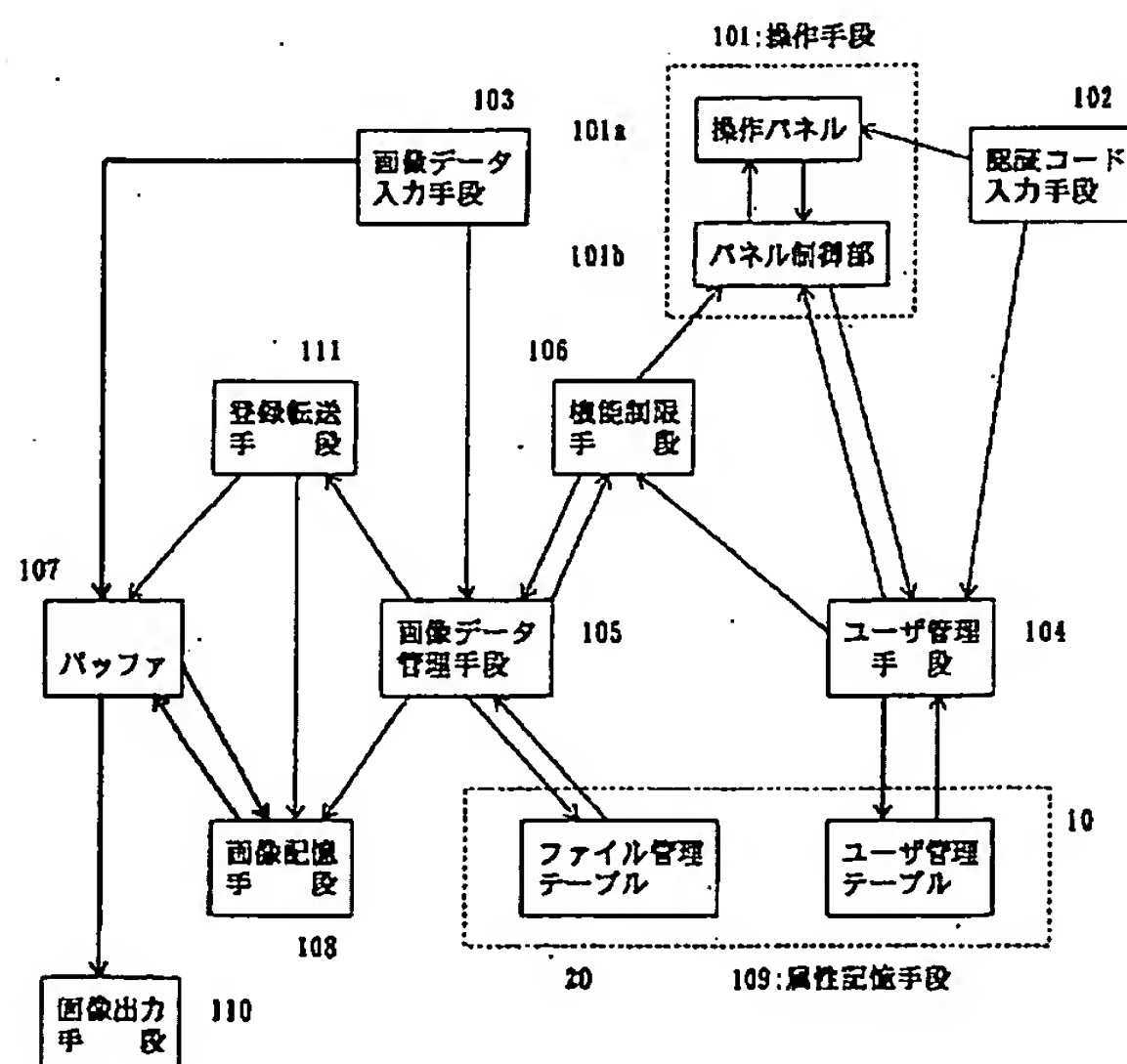
最終頁に続く

(54) 【発明の名称】 画像処理装置

(57) 【要約】

【課題】 画像データの蓄積および読み出しを行う
画像処理装置に関するものである。

【解決手段】 固有の認証コードが記録されている認証用媒体より該認証コードの読み込みを行う認証コード入力手段１０２と、ユーザ登録時に発行される固有のユーザ認証番号を含むユーザＩＤ情報の入力を行うユーザＩＤ入力手段と、上記認証コード、および上記ユーザＩＤ情報に基づいてユーザを管理するユーザ管理手段１０４と、上記認証コード入力手段１０２より入力された上記認証コードまたは上記ユーザＩＤ入力手段より入力された上記ユーザＩＤ情報に基づいてユーザを特定できない場合に、上記ユーザが使用できる機能の範囲を制限する機能制限手段１０６とを備える。よって、不特定のユーザによる画像データの蓄積を防止することができ、また、蓄積されている画像データの機密性を確保することができる。



(2)

1

【特許請求の範囲】

【請求項1】 入力された画像データを画像記憶手段に蓄積し、該入力された画像データ、または上記画像記憶手段に蓄積されている画像データを画像出力手段により出力する画像処理装置において、

固有の認証コードが記録されている認証用媒体より該認証コードの読み込みを行う認証コード入力手段と、

ユーザ登録時に発行される固有のユーザ認証番号を含むユーザID情報の入力を行うユーザID入力手段と、

上記認証コード、および上記ユーザID情報に基づいてユーザを管理するユーザ管理手段と、

上記認証コード入力手段より入力された上記認証コードまたは上記ユーザID入力手段より入力された上記ユーザID情報に基づいてユーザを特定できない場合に、上記ユーザが使用できる機能の範囲を制限する機能制限手段とを備えたことを特徴とする画像処理装置。

【請求項2】 上記機能制限手段が、上記画像データを上記画像記憶手段へ蓄積する機能を制限する請求項1に記載の画像処理装置。

【請求項3】 上記機能制限手段が、上記画像記憶手段に蓄積された画像データを該画像記憶手段から読み出して上記画像出力手段から出力する機能を制限する請求項1または請求項2に記載の画像処理装置。

【請求項4】 入力された画像データを画像記憶手段に蓄積し、該入力された画像データ、または上記画像記憶手段に蓄積されている画像データを画像出力手段により出力する画像処理装置において、

固有の認証コードが記録されている認証用媒体より該認証コードの読み込みを行う認証コード入力手段と、

ユーザ登録時に発行される固有のユーザ認証番号を含むユーザID情報の入力を行うユーザID入力手段と、

上記認証コード、および上記ユーザID情報に基づいてユーザを管理するとともに、該ユーザが属するグループを示すグループ属性情報の管理を行うユーザ管理手段と、

上記画像データと、該画像データを登録したユーザおよび上記画像記憶手段へのアクセス可能範囲を示す該画像データのアクセス権情報とを関連付けて管理する画像データ管理手段と、

上記認証コード入力手段より入力された上記認証コードまたは上記ユーザID入力手段より入力された上記ユーザID情報に基づいて上記ユーザ管理手段が特定したユーザおよび該ユーザの上記グループ属性情報と、上記画像データ管理手段により特定された読み出し対象の画像データを登録したユーザおよび該画像データの上記アクセス権情報とに基づいて、上記画像記憶手段からの上記画像データの読み出しを制限する機能制限手段とを備えたことを特徴とする画像処理装置。

【請求項5】 上記画像データ管理手段により上記画像データに対応して管理される上記アクセス権情報が、上

2

記ユーザ管理手段により特定される該画像データを登録するユーザに対応するグループ属性情報により形成される請求項4に記載の画像処理装置。

【請求項6】 上記画像データ管理手段により上記画像データに対応して管理される上記アクセス権情報が、該画像データを登録するユーザにより設定される請求項4または請求項5に記載の画像処理装置。

【請求項7】 上記ユーザ管理手段は、上記認証コード入力手段から上記認証コード、あるいは上記ユーザID入力手段から上記ユーザID情報が入力されると、上記認証コードあるいは上記ユーザID情報に対応するすべての情報を削除する請求項1～請求項6のいずれかに記載の画像処理装置。

【請求項8】 上記ユーザ管理手段は、上記認証コード入力手段から未登録の上記認証コード、および上記ユーザID入力手段から変更を行うユーザの上記ユーザID情報が入力されると、上記ユーザID情報に対応する認証コードを上記未登録の認証コードに変更する請求項1～請求項7のいずれかに記載の画像処理装置。

【請求項9】 上記ユーザID情報が、上記ユーザ認証番号である請求項1～請求項8のいずれかに記載の画像処理装置。

【請求項10】 上記ユーザID情報が、上記ユーザ認証番号、およびパスワードである請求項1～請求項8のいずれかに記載の画像処理装置。

【請求項11】 上記ユーザ管理手段は、上記認証コード入力手段から未登録の上記認証コードが入力されると、ユーザ認証番号の発行を行い、該ユーザ認証番号をユーザに対して通知するとともに、上記認証コードおよび上記ユーザ認証番号を新規登録する請求項9に記載の画像処理装置。

【請求項12】 上記ユーザ管理手段は、上記認証コード入力手段から未登録の上記認証コードが入力されると、ユーザ認証番号の発行を行い、該ユーザ認証番号をユーザに対して通知し、更に該ユーザによって上記ユーザID入力手段からパスワードが入力されると、上記認証コード、上記ユーザ認証番号および上記パスワードを新規登録する請求項10に記載の画像処理装置。

【請求項13】 上記ユーザ管理手段は、上記認証コード入力手段から上記認証コード、あるいは上記ユーザID入力手段から上記ユーザID情報が入力され、新規のパスワードが入力されると、上記認証コードあるいは上記ユーザID情報に対応する上記パスワードを上記新規のパスワードに変更する請求項10または請求項12に記載の画像処理装置。

【請求項14】 上記認証コード入力手段は、磁気カード読取装置、パンチカード読み取り装置、またはICカード読み取り装置のいずれかである請求項1～請求項13のいずれかに記載の画像処理装置。

【請求項15】 上記ユーザID入力手段は、キーボー

3

ド、テンキー、またはタッチパネルのいずれかの入力装置、もしくは、シリアル通信手段である請求項1～請求項14のいずれかに記載の画像処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、画像データの蓄積および読み出しを行う画像処理装置に関するものである。

【0002】

【従来の技術】デジタル技術の発達により、画像データは紙へコピーとして記録するだけでなく、磁気ディスク、光ディスク、光磁気ディスク等へ画像データをファイルとして記憶することができるようになった。また、複写機分野ではプリンタ、ファクスなどの機能を組み込みデジタル複合機として成長し続けている。さらに、上記のようなファイリング機能を組み込んだデジタル複合機も商品化され始めている。しかしながら、複写機のように多数の人が共用する機器においては記録されているデータも共有する反面、あまり公にできないような内容であっても容易に取り出すことができる。この

ような問題を解決した画像複写装置が、特開平4-183175号公報に開示されている。

【0003】この画像複写装置の構成図を図13に示し、その概略について以下に説明する。まず、IDカード読み取り部205に挿入されたIDカードより記憶されている使用者管理コードを読み取り、制御回路部206のメモリ上に該使用者管理コードを記憶する。

【0004】次に、原稿台に置かれた原稿画像は、CCD201で光学的に読み込まれ電気信号に変換される。CCD201からの出力はアナログ信号処理部202において増幅され、次にデジタル信号処理部203でデジタル化されシェーディング補正などの信号処理が行われる。制御回路部206により画像データの流れがコントロールされ、画像記憶部207に読み込まれた画像データが記録される。この記録された画像データはプリンタ204により紙に印刷され、コピーが終了する。

【0005】次に、再び上記IDカード読み取り部205にIDカードが挿入され、このIDカードの使用者管理コードと、上記制御回路部206のメモリ上に記憶されている使用者管理コードとが違った場合には、上記画像記憶部207に記憶されている画像データを消去してしまう。一方、同じである場合には再コピーランプを点灯し、上記画像記憶部207に記憶されている上記画像データを再び印刷できることを利用者に通知する。利用者が再コピーを選択すると、上記画像記憶部207に記憶されている画像データをプリンタ部204により出力する。

【0006】

【発明が解決しようとする課題】以上のように、上記のような画像複写装置によれば上記画像記憶部207に記

(3)

4

憶されている画像データについて、使用者管理コードが異なるIDカードが使用された場合に上記画像データを消去するので、該画像データの機密性を高めることができる。しかしながら、上記のように、現在上記制御回路部206のメモリ上に記憶されている使用者管理コード以外の利用者が使用すると上記画像記憶部207の画像データが消去されてしまうので、その後使用者管理コードが同一の利用者が画像記憶部の画像データを取り出そうとしても、該当する画像データはなくなってしまっており、取り出すことができない。

【0007】また、ネットワークを利用するコンピュータの分野などでは、ユーザを限定する手法として、古くからユーザIDとパスワードを入力してその使用範囲を限定するといった手法が用いられている。

【0008】しかしながら、このようにIDとパスワードを用いて装置を使うというコンピュータの分野では普通の方法であっても、複写機のように操作上の入力手段の乏しいOA機器では、操作が煩雑な上、コンピュータに慣れていない利用者にとっては抵抗を感じるようである。更に、従来磁気カードなどを利用して機器の使用を制限している複写機も開発されているが、これは課金を目的としており、カードさえ持っていれば、ほとんど制限なくその機器は使用できてしまう。そのため、現在のような機密性が要求されるシステムにはそのまま使用できない。

【0009】本発明は上記の事情に鑑みて提案されたものであって、操作性が煩雑にならずに記録されている画像データの機密性を高めることができる画像処理装置を提供することを目的とする。

【0010】

【課題を解決するための手段】本発明は上記目的を達成するために以下の手段を採用している。まず、本発明は、入力された画像データを画像記憶手段108に蓄積し、該入力された画像データ、または上記画像記憶手段108に蓄積されている画像データを画像出力手段110により出力する画像処理装置を前提としている。

【0011】上記画像処理装置において、本発明は固有の認証コードが記録されている認証用媒体より該認証コードの読み込みを行う認証コード入力手段102と、ユーザ登録時に発行される固有のユーザ認証番号を含むユーザID情報の入力を行うユーザID入力手段と、上記認証コード、および上記ユーザID情報に基づいてユーザを管理するユーザ管理手段104と、上記認証コード入力手段102より入力された上記認証コードまたは上記ユーザID入力手段より入力された上記ユーザID情報に基づいてユーザを特定できない場合に、上記ユーザが使用できる機能の範囲を制限する機能制限手段106とを備えた構成としている。

【0012】また、上記機能制限手段106により、上記画像データを上記画像記憶手段108へ蓄積する機能

5

を制限することができる。更に、上記画像記憶手段108に蓄積された画像データを該画像記憶手段108から読み出して上記画像出力手段110から出力する機能を制限することができる。

【0013】このことにより、上記認証用媒体が手元にならないような場合であっても上記ユーザID入力手段からユーザ認証番号を入力することにより、ユーザを特定することができる。また、ユーザが登録されていない場合、上記画像処理装置の使用を制限することができる。よって、不特定のユーザによる画像データの蓄積を防止

【0014】また、上記画像処理装置において、固有の認証コードが記録されている認証用媒体より該認証コードの読み込みを行う認証コード入力手段102と、ユーザ登録時に発行される固有のユーザ認証番号を含むユーザID情報の入力を行うユーザID入力手段と、上記認証コード、および上記ユーザID情報に基づいてユーザを管理するとともに、該ユーザが属するグループを示すグループ属性情報の管理を行うユーザ管理手段104と、上記画像データと、該画像データを登録したユーザおよび上記画像記憶手段108へのアクセス可能範囲を示す該画像データのアクセス権情報とを関連付けて管理する画像データ管理手段105と、上記認証コード入力手段102より入力された上記認証コードまたは上記ユーザID入力手段より入力された上記ユーザID情報に基づいて上記ユーザ管理手段104が特定したユーザおよび該ユーザの上記グループ属性情報と、上記画像データ管理手段105により特定された読み出し対象の画像データを登録したユーザおよび該画像データの上記アクセス権情報とに基づいて、上記画像記憶手段からの上記画像データの読み出しを制限する機能制限手段106とを備えた構成としている。

【0015】上記画像データ管理手段105により上記画像データに対応して管理される上記アクセス権情報は、上記ユーザ管理手段104により特定される該画像データを登録するユーザに対応するグループ属性情報により形成される。また、該画像データを登録するユーザが必要に応じて設定することもできる。

【0016】このことにより、上記画像データを単位として読み出しを制限しているので、蓄積されている画像データの機密性を効率的に高めることができる。

【0017】

【発明の実施の形態】

(実施例1) 図1は本発明の一実施例における画像処理装置の構成を示す機能ブロック図であり、図2は動作手順を示すフローチャートであり、以下図に基づいて構成とともに動作を説明する。

【0018】まず、ユーザは、例えば磁気カードリーダー等の認証コード入力手段102に、カード毎にユニーク

(4)

6

な認証コードが記録された磁気カード等の認証用媒体を挿入するか、あるいは、タッチパネル付きLCDパネルもしくはテンキーなどの複数のキーを備えた操作手段101の操作パネル101aを用いて、ユーザ認証番号の入力を行う(図2、ステップS101)。

【0019】上記のように上記認証用媒体が挿入された場合、上記認証コード入力手段102は上記認証用媒体に記録されている上記認証コードを読み出し、ユーザ管理手段104に通知する。一方、上記操作パネル101aを用いて上記ユーザ認証番号の入力が行われた場合、該ユーザ認証番号は上記操作手段101のパネル制御部101bに保持され、該パネル制御部101bは上記操作パネル101aの実行ボタンが押下されると、上記ユーザ認証番号をユーザ管理手段104に通知する。

【0020】該ユーザ管理手段104は、以下に説明するようなユーザ管理テーブル10を用いてユーザの管理を行っており、上記のように上記認証コード入力手段102から上記認証コードが通知されるか、あるいは上記操作手段101から上記ユーザ認証番号が通知されると、上記ユーザ管理テーブル10をアクセスすることによって上記認証コードもしくは上記ユーザ認証番号がユーザ登録されているかどうかの判断を行い、この判断結果を機能制限手段106に通知する(ステップS102)。

【0021】上記ユーザ管理テーブル10は、例えば図3に示すように、上記認証用媒体に記録されている上記認証コード11、ユーザ登録時に発行するユーザに固有の番号であるユーザ認証番号12、登録されているユーザの名称を識別できるように名前やニックネーム等で表されるユーザ名13、例えばハードディスク等の画像記憶手段108にユーザが登録された日付を示す登録日14等により構成されている。尚、上記認証コード11は上記認証用媒体に記録されているので桁数の多いコードでよく、また、上記ユーザ認証番号12は、利用者が上記操作パネル101aから入力するためにできるだけ簡単に桁数が少ない方が望ましい。

【0022】次に、上記ユーザ管理手段104より通知された上記判断結果がユーザ登録されているとの判断である場合、上記機能制限手段106は動作許可を発行し、画像データ管理手段105および上記パネル制御部101bに対して通知する。この動作許可の通知を受けた該パネル制御部101bは上記操作パネル101aの実行ボタンのLEDを赤色から緑色に変化させる等により、使用可能状態であることをユーザに通知する(ステップS103)。

【0023】一方、上記ユーザ管理手段104より通知された上記判断結果がユーザ登録されていないとの判断である場合、上記機能制限手段106は動作許可の発行を行わず、上記画像データ管理手段105および上記パネル制御部101bに対して動作不許可を通知する。こ

(5)

7

の動作不許可の通知を受けた該パネル制御部101bは、上記操作パネル101aにユーザ未登録である旨を表示する（ステップS108）。

【0024】また、上記認証コード入力手段102は、上記認証用媒体が裏向きに挿入されたり、違う種類の認証用媒体が挿入された場合に、認証用媒体の誤挿入を上記パネル制御部101bに通知し、該パネル制御部101bは上記操作パネル101aに認証用媒体誤挿入である旨を表示する。

【0025】上記のようにして使用可能状態になると、ユーザは上記操作パネル101aから実行したい動作を選択する（ステップS104）。本実施例において、ユーザが実行する動作の第1は、原稿画像を光学的に読み取るイメージスキャナ等の画像データ入力手段103で読み込み、読み込まれた原稿画像の画像データを、デジタル化して上記画像記憶手段108に記憶するファイリング動作である（ステップS105）。第2は、上記画像データ入力手段103で読み込んだ画像データを例えば電子写真方式のプリンタ等の画像出力手段110から紙やOHPシートなどの媒体に印刷するコピー動作である（ステップS106）。第3は、上記画像記憶手段108にファイリングされている画像データを上記画像出力手段110から出力するファイル出力動作である（ステップS107）。

【0026】次に、上記操作パネル101aより選択された上記動作が入力されると、この動作指示は上記パネル制御部101bに保持され、該パネル制御部101bは上記操作パネル101aの実行ボタンが押下されると、上記機能制限手段106の動作許可に基づいて、上記画像データ管理手段105に通知される。該画像データ管理手段105では、上記動作指示の内容に従った処理動作を行う。

【0027】以上のように、本実施例の画像処理装置では、上記認証コード入力手段102と上記ユーザID入力手段とを設けることにより、上記認証用媒体が手元にないような場合であっても上記操作パネル101aからユーザ認証番号を入力することにより、ユーザを特定することができる。また、上記ユーザ管理手段104に登録されていないユーザの場合は装置の利用を排除することができる。

【0028】なお、本実施例ではすべての機能を拒絶するような制限を設けた場合について説明しているが、上記ファイリング動作と上記ファイル出力動作のように、上記画像記憶手段108へのアクセスが伴うような動作に限定して制限することも可能であり、この場合も上記画像記憶手段108の機密性を高めることができる。更に、上記画像記憶手段108へのアクセスする機能に限らず、任意の機能に限定して制限を行うことも可能である。

【0029】また、上記操作手段101は、上記操作パ

8

ネル101aよりユーザ認証番号を入力することによりユーザID入力手段として機能する。更に、上記操作パネル101aの入力部は、コピー枚数やソータの制御といったパラメータ、あるいはコピーやファイリングといった動作モードを選択する。上記操作パネル101aの表示部は、画像処理装置の状態や、エラーメッセージなどを利用者に伝達する機能を備えている。

【0030】上記実施例において、上記認証用媒体に記録する上記認証コードを各認証用媒体で連続するように構成することも可能であり、この場合ユニークな上記認証用媒体を容易に作成することができる上、作成した上記認証用媒体の管理も非常に容易になる。ここで、この認証用媒体毎にユニークでかつ連続した認証コードを記録する手順について説明する。

【0031】まず、1枚目に記録したい認証コードの初期値を入力する（図4、ステップS201）。認証コードを記録する認証用媒体をライターに挿入すると（ステップS202）、認証コードが書き込まれる（ステップS203）。この書き込まれた認証コードを確認すると（ステップS204）、認証用媒体が排出される（ステップS205）。さらに記録したい認証用媒体がある場合には、認証コードが1つ更新され（ステップS206→S207）、上記ライターへの認証用媒体の挿入待ちになる。このように、非常に簡単なシーケンスで連続した認証コードの認証用媒体を作成することができる。

【0032】また、上記実施例の画像処理装置において、ファクシミリ送受信機能を備えた場合やパソコンなどからのプリントアウト機能を備えたような画像処理装置であっても上記と同様の機能を実現することができる。

【0033】なお、原稿画像は、人の目またはOCRなどの人工的な目に対して一定の情報を与えるイメージ情報であり、例えば紙、プラスチックシート、プラスチックフィルム等に印刷された文字、数字、図、写真等全てを含むものとする。

【0034】（実施例2）本発明の他の実施例における画像処理装置での画像データのファイリング（蓄積）について、以下図に基づいて構成とともに動作を説明する。尚、主な構成は上記実施例1と同様であるので図1を用いて説明し、同様の構成については説明を省略する。

【0035】まず、ユーザは上記実施例1と同様に、上記認証コード入力手段102に上記認証用媒体を挿入するか、あるいは、上記操作パネル101aを用いて上記ユーザ認証番号の入力を行う（図5、ステップS301）。

【0036】上記のように上記認証用媒体が挿入された場合、上記認証コード入力手段102は上記認証用媒体に記録されている上記認証コードを読み出し、ユーザ管理手段104に通知する。一方、上記操作パネル101

50

9

aを用いて上記ユーザ認証番号の入力が行われた場合、該ユーザ認証番号は上記操作手段101のパネル制御部101bに保持され、該パネル制御部101bは上記操作パネル101aの実行ボタンが押下されると、上記ユーザ認証番号をユーザ管理手段104に通知する。

【0037】次に、上記ユーザ管理手段104は、上記のように上記認証コード入力手段102から上記認証コードが通知されるか、あるいは上記操作手段101から上記ユーザ認証番号が通知されると、上記ユーザ管理テーブル10をアクセスすることによって上記認証コードもしくは上記ユーザ認証番号がユーザ登録されているかどうかの判断を行い、この判断結果を上記機能制限手段106に通知する（ステップS302）。

【0038】ここで、上記ユーザ管理テーブル10は、例えば図6に示すように上記実施例1の構成に加えて、ユーザがどのグループに属しているかを示すグループ属性情報15を管理している。上記ユーザ管理手段104は、上記判断結果がユーザ登録されているとの判断である場合、上記判断結果に加えて上記ユーザのユーザ認証番号12および該ユーザに応じた上記グループ属性情報15を機能制限手段106に通知する。

【0039】次に、上記機能制限手段106は、上記ユーザ管理手段104より通知された上記判断結果がユーザ登録されているとの判断である場合、上記実施例1と同様にして、上記機能制限手段106による動作許可の発行等がなされ、使用可能状態であることがユーザに通知される（ステップS303）。

【0040】一方、上記ユーザ管理手段104より通知された上記判断結果がユーザ登録されていないとの判断である場合、上記機能制限手段106は上記ファイリング動作についての動作許可の発行を行わず、上記画像データ管理手段105および上記パネル制御部101bに対してこの旨通知する。この動作不許可の通知を受けた該パネル制御部101bは、上記操作パネル101aにこのファイリング動作不許可である旨を表示する（ステップS310）。

【0041】上記のようにして使用可能状態になると、ユーザは上記操作パネル101aから実行したい動作（本実施例ではファイリング動作）を選択して入力する（ステップS304）。この時、この動作指示は上記パネル制御部101bに保持され、該パネル制御部101bは上記操作パネル101aの実行ボタンが押下されると、上記機能制限手段106の動作許可に基づいて、上記画像データ入力手段103に対して原稿の読み込みの指示を与え、また上記画像データ管理手段105に対して上記画像データのファイリングの指示を与える（ステップS305）。

【0042】上記指示を受けた上記画像データ入力手段103は原稿を読み込み、デジタル変換して画像データとしてバッファ104に格納する（ステップS30

(6)

10

6）。同時に、上記画像データのファイリングの指示を受けた上記画像データ管理手段105は、これからファイリングする画像データに対応する画像IDを生成する（ステップS307）。

【0043】次に、登録転送手段111が、上記画像データ管理手段105より受けた上記画像IDに基づいたファイル名を付して、上記バッファ104に格納された上記画像データを上記画像記憶手段108に蓄積する（ステップS308）。

10 【0044】この時、上記画像データ管理手段105は、上記蓄積する画像データに対応した上記ファイル名21、該画像データが登録された日付を示す登録日22、以下に説明する登録者23、およびアクセス権情報24等の情報を、例えば図7に示すような上記属性記憶手段109のファイル管理テーブル20に記憶する（ステップS309）。

20 【0045】上記画像データを登録したユーザを示す上記登録者23は、上記ユーザ管理手段104により特定され上記機能制限手段106に通知された上記ユーザ認証番号12が上記ファイル管理テーブル20に記憶される。

30 【0046】また、上記画像記憶手段108へのアクセス可能範囲を示す上記アクセス権情報24は、上記ユーザ認証番号とともに上記機能制限手段106に通知された上記グループ属性情報15が通常そのまま反映され、上記ファイル管理テーブル20に記憶される。ここで、上記アクセス権情報の設定を行うことも可能であり、例えば、画像データを登録するユーザが自身の属するグループに加えて他のグループに対しても該画像データを公開できるように指定する場合、利用者全員に画像データを公開できるように指定する場合、画像データを登録するユーザ以外には公開できないように指定する場合等を選択して、上記ファイリング動作の指示時等に上記操作パネル101aより入力を行うことができる。

40 【0047】この場合の上記アクセス権情報24について、グループAに属するユーザが画像データを登録するものとして、以下説明する。指定のない場合、上記アクセス権情報24はユーザの属するグループAとなる（図7、①参照）。ユーザが自身の属するグループに加えて他のグループ（Cとする）に対しても該画像データを公開できるように指定した場合、上記アクセス権情報24はユーザの属するグループAおよび追加したグループCとなる（図7、②参照）。次に、利用者全員に画像データを公開できるように指定した場合、上記アクセス権情報24はユーザの属するグループAおよびALLとなる（図7、③参照）。また、画像データを登録するユーザ以外には公開できないように指定した場合、上記アクセス権情報24はユーザの属するグループAが削除され、グループ属性のない状態となる（図7、④参照）。

50 【0048】また、上記のように設定された上記アクセ

11

ス権情報24を、上記画像データが一旦ファイリングされた後であっても必要に応じて変更できるような構成とすることも可能である。

【0049】（実施例3）上記実施例2に記載の画像処理装置において、上記画像IDにより画像データを指定し、該画像データを読み出す動作を以下説明する。図8はこの動作を示すフローチャートである。

【0050】まず、ユーザは上記実施例2と同様に、上記認証コード入力手段102に上記認証用媒体を挿入するか、あるいは、上記操作パネル101aを用いて上記ユーザ認証番号の入力を行う。

【0051】以降、上記ユーザ管理手段104によるユーザの特定、上記機能制限手段106による動作許可の発行等については、上記実施例2と同様にして行われる。上記のようにして使用可能状態になると、ユーザは上記操作パネル101aから実行したい動作（本実施例ではファイル出力動作）を選択して、読み出したい画像データの画像IDを入力する（図8、ステップS401）。この時、この動作指示および上記画像IDは上記パネル制御部101bに保持され、該パネル制御部101bは上記操作パネル101aの実行ボタンが押下されると、上記機能制限手段106の動作許可に基づいて、上記画像データ管理手段105に対して上記画像IDの通知および読み出し指示が行われる（ステップS402）。

【0052】上記画像データ管理手段105は、上記ファイル管理テーブル20にアクセスし、上記画像IDに対応した登録者23、およびアクセス権情報24を読み出し上記機能制限手段106に通知する（ステップS403）。

【0053】該機能制限手段106は、上記画像データ管理手段105より通知されたこの読み出し対象の画像データに対応した登録者23およびアクセス権情報24と、上記ユーザ管理手段104より通知された上記ユーザの上記ユーザ認証番号および上記グループ属性情報とに基づいて、上記画像データの読み出しを許可するか否かの判断を行う（ステップS404）。すなわち、上記ユーザの上記グループ属性情報に含まれるグループが上記画像データのアクセス権情報24に存在していれば、上記画像データの読み出し許可を与え、上記ユーザの上記グループ属性情報に含まれるグループが上記画像データのアクセス権情報24に存在していなければ、上記画像データの読み出し許可を与えない。ただし、上記ユーザの上記グループ属性情報に含まれるグループが上記画像データのアクセス権情報24に存在していなくても、上記ユーザ認証番号が上記画像データの登録者23と一致すれば、上記画像データの読み出し許可を与える。

【0054】例えば、上記アクセス権情報24がグループAだけである画像データ（図7、①参照）を読み出すことができるユーザは、上記グループ属性情報にグルー

(7)

12

プAを有するユーザであり、例えば図6においてはユーザ①、②である。ここで、ユーザ③は上記グループ属性情報にグループAを有していないので、上記画像データを読み出すことができない。

【0055】上記アクセス権情報24にALL有する画像データ（図7、③参照）は、利用者全員誰でも該画像データを読み出すことができる。また、上記アクセス権情報24がグループ属性のない状態である画像データ

（図7、④参照）を読み出すことができるユーザは、該画像データを登録したユーザだけとなる。よって、このユーザ以外は該画像データを読み出すことができない。

【0056】上記判断で上記画像データの読み出しが許可されると、上記画像データ管理手段105は、上記画像IDに対応する画像ファイルの読み出しを登録転送手段111に指示する（ステップS405）。該指示により、該登録転送手段111は上記画像ファイルの画像データを上記画像記憶手段108より上記バッファ104へ読み出し、更にこのように読み出された上記画像データは上記画像出力手段110から出力される（ステップS406）。

【0057】一方、上記判断で上記画像データの読み出しが許可されない場合、上記パネル制御部101bに通知され、該パネル制御部101bは、上記操作パネル101aに上記画像データの読み出しが許可されない旨を表示する（ステップS407）。

【0058】以上のように、上記画像データのアクセス権情報と上記ユーザの上記グループ属性情報に基づいて上記画像データを単位として読み出しを制限することにより、上記画像記憶手段108に蓄積された画像データの機密性を効率的に高めることができる。

【0059】（実施例4）上記各実施例に記載の画像処理装置において、新規ユーザ登録動作について以下説明する。図9はこの動作を示すフローチャートである。

【0060】まず、登録されていない認証用媒体8を上記認証コード入力手段102に挿入する（図9、ステップS501）。上記認証コード入力手段102は上記認証用媒体に記録されている上記認証コードを読み出し、上記ユーザ管理手段104に通知する。該ユーザ管理手段104では通知された上記認証コードで上記ユーザ管理テーブル10をアクセスすることによって、上記挿入された認証用媒体8が既に登録されているか否かを確認する（ステップS502）。既に登録されている場合には、二重登録になってしまうため、その旨を上記操作パネル101aに表示しユーザに通知する。同時に上記認証用媒体8を排出し（ステップS503）、初期状態に戻り登録されていない認証用媒体の挿入を促す。

【0061】一方、上記挿入された認証用媒体が上記ユーザ管理テーブル10に登録されていない場合には、上記ユーザ管理手段104は新しいユーザ認証番号を発行しユーザに通知する（ステップS504）。新しい認証

(8)

13

番号が通知されたユーザは、上記操作パネル101aを用いて、グループ属性情報等を入力する（ステップS505）。同時に、上記ユーザ管理手段104は、新しいユーザ認証番号と上記認証コード、グループ属性情報等を関連付けて、上記ユーザ管理テーブル10に記憶する。以上の操作が終了すると上記認証用媒体8を排出し（ステップS506）、新規ユーザ登録動作を終了する（ステップS507）。

【0062】以上のように、上記認証用媒体に記憶されている上記認証コードが、上記ユーザ管理テーブル10に登録されていないと、容易に新規ユーザとして登録することができる。そのため、手元に磁気カードライタ等がなくても、あらかじめ任意のユニークな認証コードが記録されている媒体を購入することで、専用の設備を用意する必要がなくなる。

【0063】なお、本実施例では挿入した認証用媒体が既に登録されている場合には初期状態に戻るよう説明しているが、登録動作を終了してしまうこともできる。また、通常に登録された後、登録動作を終了せず、次の登録にそなえて初期状態に戻るようにすることも可能である。

【0064】（実施例5）上記各実施例に記載の画像処理装置において、ユーザ抹消動作について以下説明する。図10はこの動作を示すフローチャートである。

【0065】まず、抹消したいユーザの認証用媒体8を上記認証コード入力手段102に挿入する（図10、ステップS601）。上記認証コード入力手段102は上記認証用媒体に記録されている上記認証コードを読み出し、上記ユーザ管理手段104に通知する。該ユーザ管理手段104では通知された上記認証コードで上記ユーザ管理テーブル10をアクセスすることによって、上記挿入された認証用媒体8が既に登録されているか否かを確認する（ステップS602）。上記挿入された認証用媒体8が既に登録されていない場合には、その旨を上記操作パネル101aに表示しユーザに通知する。同時に上記認証用媒体8を排出し（ステップS603）、初期状態に戻る。

【0066】一方、上記挿入された認証用媒体が上記ユーザ管理テーブル10に登録されている場合には、上記操作パネル101aに該当するユーザを抹消する旨を表示し、ユーザに確認を促す。抹消することが確認されたら（ステップS604）、上記ユーザ管理手段104は登録されている抹消されるユーザに関する情報をすべて消去する（ステップS605）。以上の操作が終了すると認証用媒体8を排出し（ステップS606）、ユーザ抹消動作を終了する（ステップS607）。

【0067】以上のように、登録されたユーザを抹消する場合には、上記ユーザ管理テーブル10に登録されたデータを抹消するので、抹消されたユーザに使用されていた認証用媒体は、上記実施例4に示す手順にしたがっ

14

てそのまま別のユーザとして新規に登録することができる。

【0068】なお、本実施例では挿入した認証用媒体が登録されていない場合には初期状態に戻るよう説明しているが、抹消動作を終了してしまうこともできる。また、登録抹消を確認する段階（ステップS604）で確認されなかった場合に抹消動作を終了するように説明しているが、抹消動作の初期状態に戻るようにすることもできる。更に、通常に抹消された後、抹消動作を終了せず、次の抹消にそなえて初期状態に戻るようにすることも可能である。

【0069】（実施例6）上記各実施例に記載の画像処理装置において、カード変更動作について以下説明する。図11はこの動作を示すフローチャートである。

【0070】認証用媒体を紛失してしまった場合など、既に登録されているユーザの認証用媒体を変更したい場合、まず、登録されていない認証用媒体8を上記認証コード入力手段102に挿入する（図11、ステップS701）。上記認証コード入力手段102は上記認証用媒体に記録されている上記認証コードを読み出し、上記ユーザ管理手段104に通知する。該ユーザ管理手段104では通知された上記認証コードで上記ユーザ管理テーブル10をアクセスすることによって、上記挿入された認証用媒体8が既に登録されているか否かを確認する（ステップS702）。既に登録されている場合には、その旨を上記操作パネル101aに表示し、上記認証用媒体8を排出し（ステップS703）、初期状態に戻る。

【0071】一方、上記挿入された認証用媒体が上記ユーザ管理テーブル10に登録されていない場合には、ユーザは上記操作パネル101aよりユーザ認証番号を入力する（ステップS704）。上記ユーザ管理手段104は、入力されたユーザ認証番号に対応するユーザの上記ユーザ管理テーブル10の内容を、図12に示すように、以前に使用されていた認証コードから現在挿入されている上記認証用媒体の認証コードに変更する（ステップS705）。以上の操作が終了すると認証用媒体8を排出し（ステップS706）、カード変更動作を終了する（ステップS707）。

【0072】以上のように、上記認証用媒体を紛失してしまったり、壊してしまったような場合であっても、以前のユーザ情報を引き継いだまま新しい認証用媒体を、容易に登録することができる。

【0073】なお、本実施例では挿入した認証用媒体が既に登録されている場合には初期状態に戻るよう説明しているが、登録変更動作を終了してしまうこともできる。また、通常に登録変更された後、登録変更動作を終了せず、次の登録変更の登録にそなえて初期状態に戻るようにすることも可能である。

【0074】また、上記各実施例で上記操作パネル10

(9)

15

1 a から上記ユーザ認証番号を入力するものとしたが、該ユーザ認証番号に加えてパスワードを入力する構成とすることもでき、この場合、他人のユーザ認証番号を使用して容易に上記画像処理装置を使用することを防ぐことができる。尚、ユーザ認証番号に加えてパスワードを入力する構成とする場合、上記ユーザ管理テーブル10を上記ユーザ認証番号に対応してパスワードを持つ構成とする必要がある。

【0075】更に、上記パスワードをユーザが自由に変えられるようにすることも可能であり、例えばあらかじめ装置管理者がパスワードを入力した場合等に、該パスワードを自分の理解しやすいものに変更することができる。以下に、上記パスワードを変更する手順の一例を簡単に説明する。まず、上記認証コード入力手段102に上記認証用媒体を挿入するか、あるいは、上記操作パネル101aを用いて上記ユーザ認証番号およびパスワードの入力を行う。次にパスワード変更機能を選択し、上記操作パネル101aを用いて現在使用中のパスワードを入力する。次に、新しく使用したいパスワードを入力する。上記ユーザ管理手段104では、上記ユーザ管理テーブル10をアクセスし、上記認証コードもしくは上記ユーザ認証番号に対応するパスワードを変更する。このようにして、パスワードを容易に変更することができる。

【0076】ところで、上記認証コード入力手段102は、磁気カードリーダーの他に、パンチカード読み取り装置、ICカード読み取り装置などのカード毎にユニークな認証コードをつけることができる媒体を用いるような装置であれば同様の効果が得られる。

【0077】また、上記実施例では、上記ユーザID入力手段を上記操作パネル101aを備えた上記操作手段101として説明しているが、これは、キーボード、テンキー、タッチパネルなどの入力装置であれば同様の効果が得られる。また、LAN、IrDA、RS232Cなどのシリアル通信手段を使用すればリモートで 사용할こともできる。

【0078】

【発明の効果】以上のように本発明に係る画像処理装置によれば、上記認証コード入力手段と上記ユーザID入力手段とを設けることにより、上記認証用媒体が手元にないような場合であっても上記ユーザID入力手段からユーザ認証番号を入力することにより、ユーザを特定することができる。また、ユーザを特定することができない場合、画像処理装置の使用を制限することができる。

【0079】また、読み出し対象の画像データのアクセ

16

ス権情報と読み出そうとするユーザのグループ属性情報に基づいて、上記画像データを単位として読み出しを制限しているため、蓄積されている画像データの機密性を効率的に高めることができる。

【0080】また、新規ユーザ登録、登録ユーザの抹消、登録カードの変更を容易に行うことができ、認証用媒体は使い回しすることもできる。

【図面の簡単な説明】

【図1】本発明の一実施例の構成を示すブロック図である。

【図2】本発明の一実施例における動作手順を示すフローチャートである。

【図3】本発明のユーザ管理テーブルの一例を示す概念図である。

【図4】認証用媒体への認証コードの記録手順を示すフローチャートである。

【図5】本発明の一実施例における画像データのファイリング時の動作手順を示すフローチャートである。

【図6】本発明のユーザ管理テーブルの一例を示す概念図である。

【図7】本発明のファイル管理テーブルの一例を示す概念図である。

【図8】本発明の一実施例における画像データの読み出し時の動作手順を示すフローチャートである。

【図9】本発明の一実施例における新規ユーザ登録手順を示すフローチャートである。

【図10】本発明の一実施例におけるユーザ抹消手順を示すフローチャートである。

【図11】本発明の一実施例における登録カード変更手順を示すフローチャートである。

【図12】本発明の一実施例における登録カード変更時のユーザ管理テーブルの一例を示す概念図である。

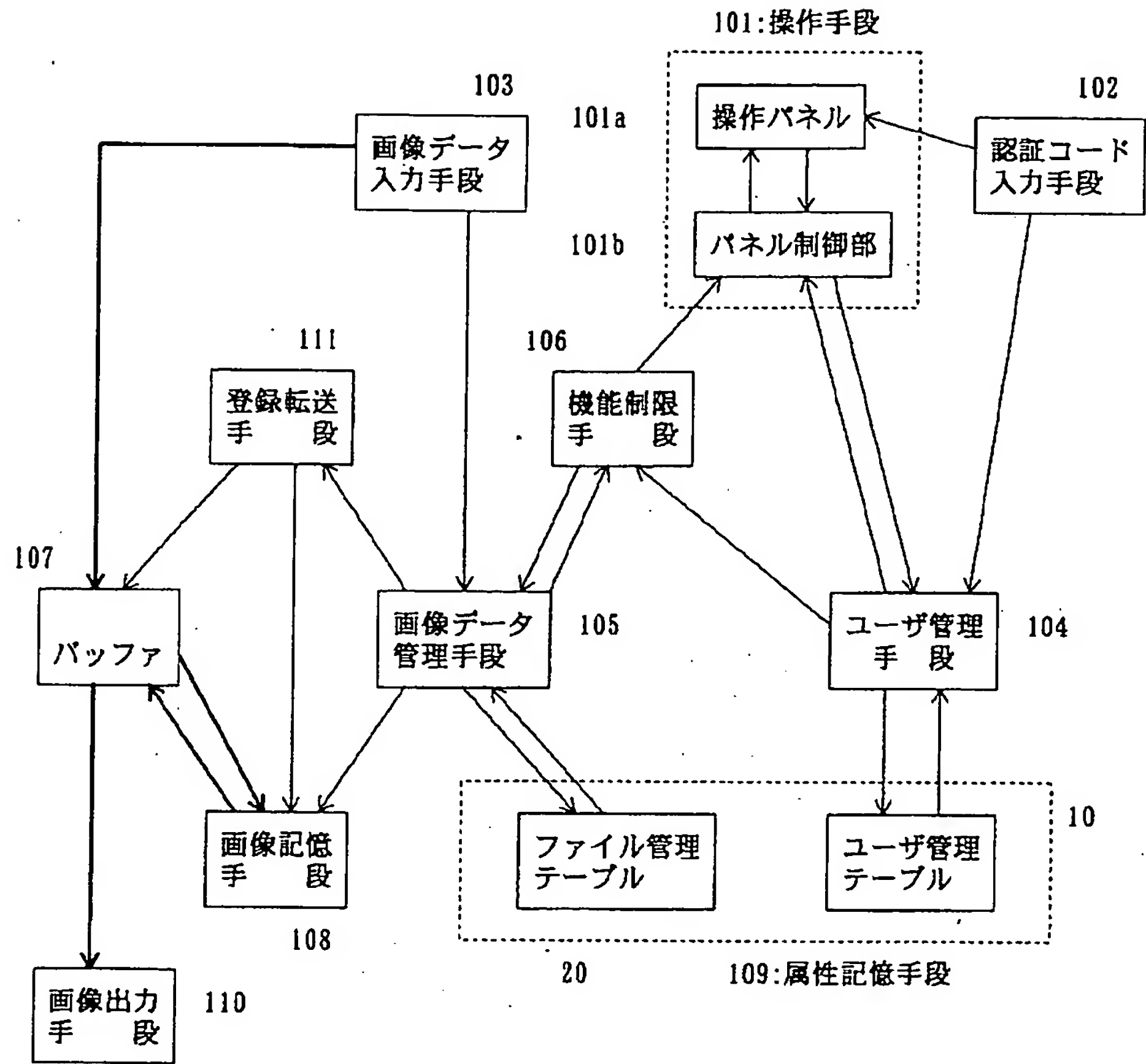
【図13】画像複写装置の従来例を示す構成図である。

【符号の説明】

- 101 操作手段
- 102 認証コード入力手段
- 103 画像データ入力手段
- 104 ユーザ管理手段
- 105 画像データ管理手段
- 106 機能制限手段
- 107 バッファ
- 108 画像記憶手段
- 109 属性記憶手段
- 110 画像出力手段

(10)

【図1】



【図3】

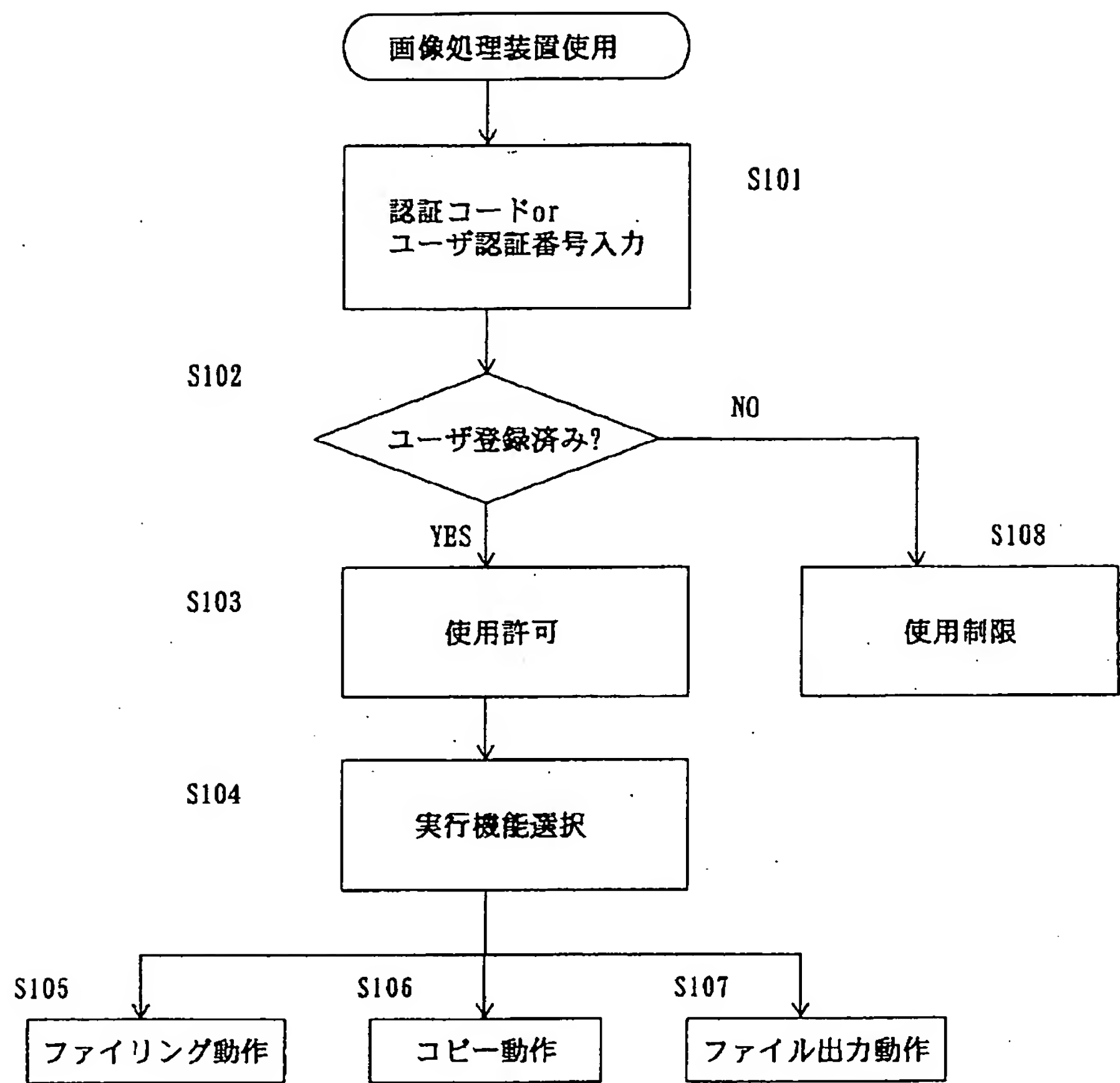
11	12	13	14
認証コード	ユーザ認証番号	使用者名	登録日
xxxxx1	1234	Micky	1996.01.08
xxxxx2	2222	Donald	1996.12.25
xxxxx3	3456	Goofy	1997.01.28
⋮	⋮	⋮	⋮

【図6】

ユーザ管理テーブル							
11	12	13	14	15			
認証コード	ユーザ認証番号	使用者名	登録日	グループ属性			
				A	B	C	
xxxxx1	1234	Micky		1	0	0	…①
xxxxx2	2222	Donald		1	0	1	…②
xxxxx3	3456	Goofy		0	1	0	…③
⋮	⋮	⋮		⋮	⋮	⋮	

(11)

【図2】



【図7】

ファイル管理テーブル

21 ファイル名	22 登録日	23 最終アクセス日	24 登録者	アクセス情報				
				A	B	C	All	
file 1	1234	1	0	0	0	...①
file 2	1234	1	0	1	0	...②
file 3	1234	1	0	0	1	...③
file 4	1234	0	0	0	0	...④
file 5	3456	0	1	0	0	...⑤
file 6	2222	1	0	1	0	...⑥
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

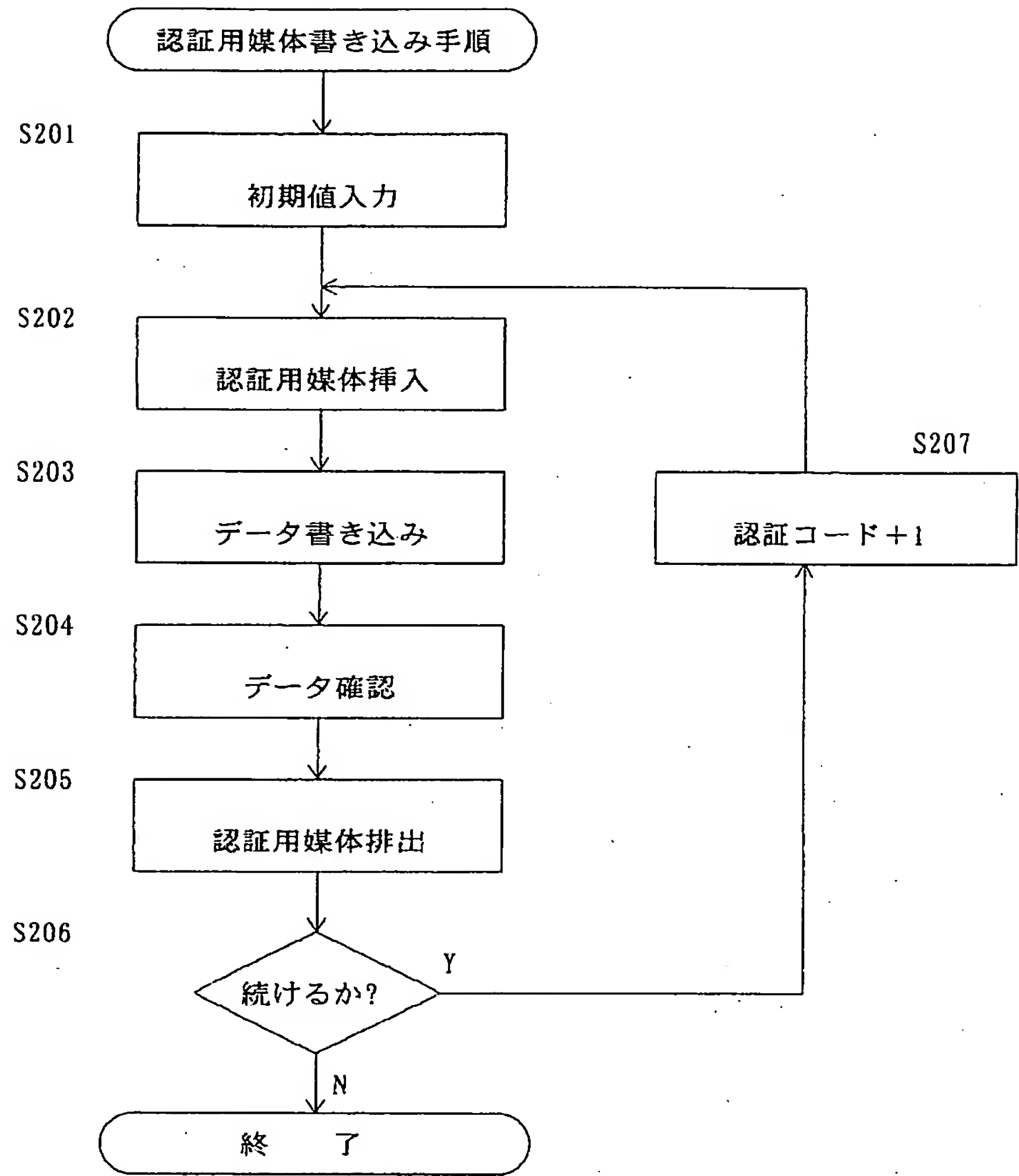
【図12】

11 認証コード	12 ユーザ認証番号	13 使用者名	14 登録日
XXXXX1	1234	Micky	1996.01.08
XXXXX2	2222	Donald	1996.12.25
XXXXX3	3456	Goofy	1997.01.28
⋮	⋮	⋮	⋮

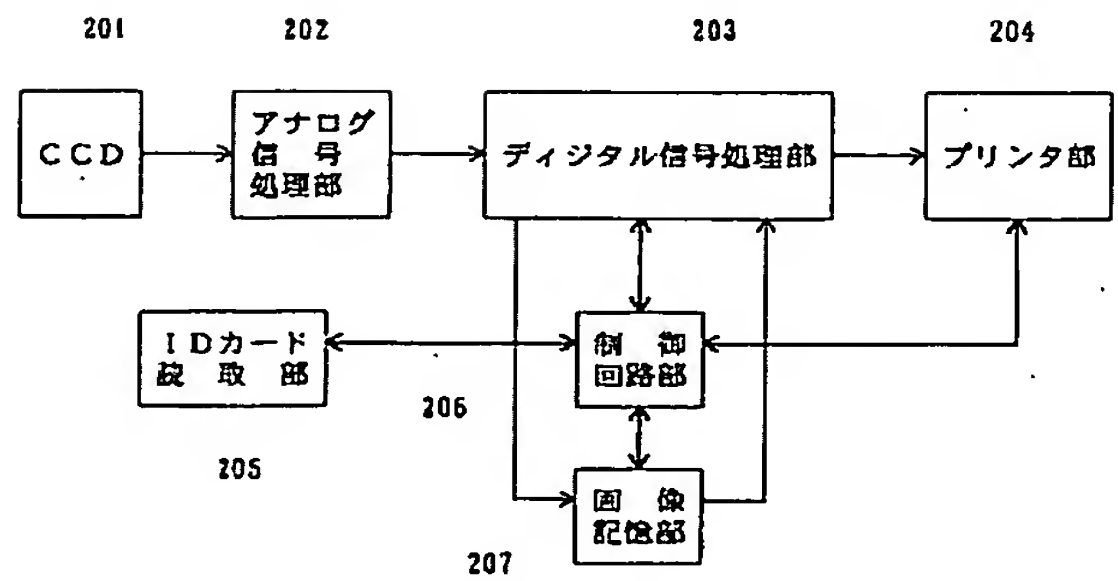
認証コード	ユーザ認証番号	使用者名	登録日
XXXXX4	1234	Micky	1996.01.08
XXXXX2	2222	Donald	1996.12.25
XXXXX3	3456	Goofy	1997.01.28
⋮	⋮	⋮	⋮

(12)

【図 4】

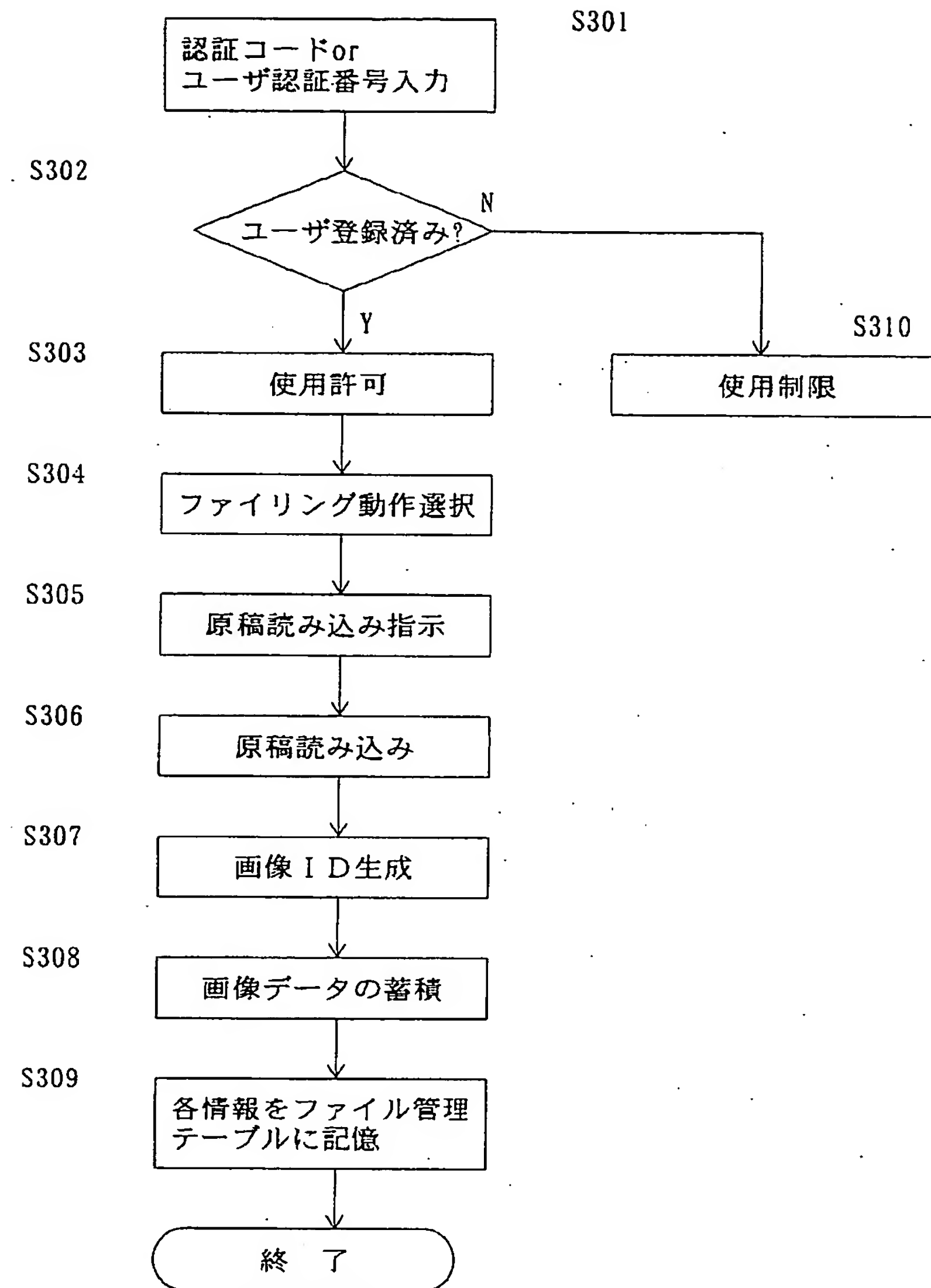


【図 1 3】



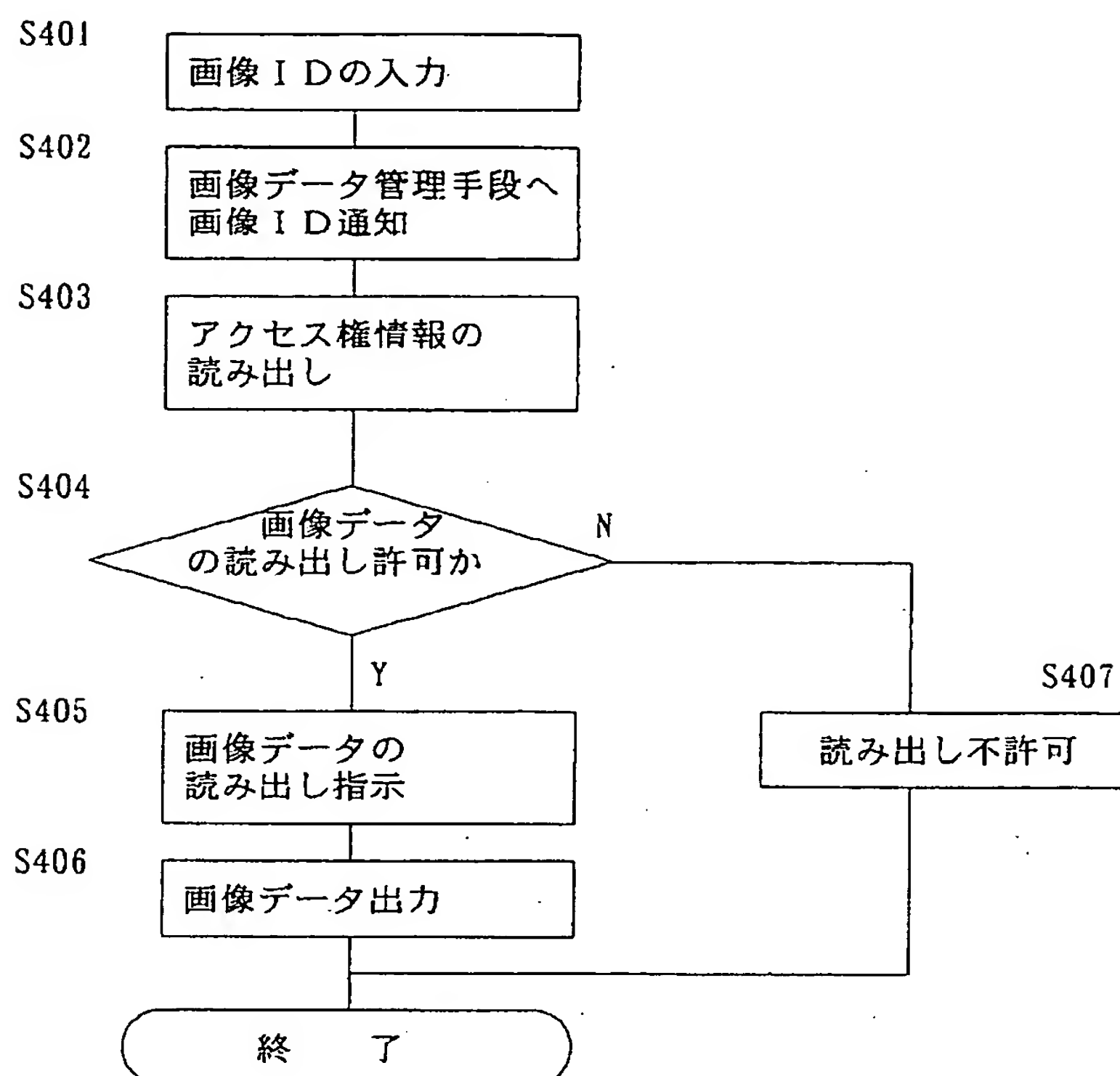
(13)

【図5】



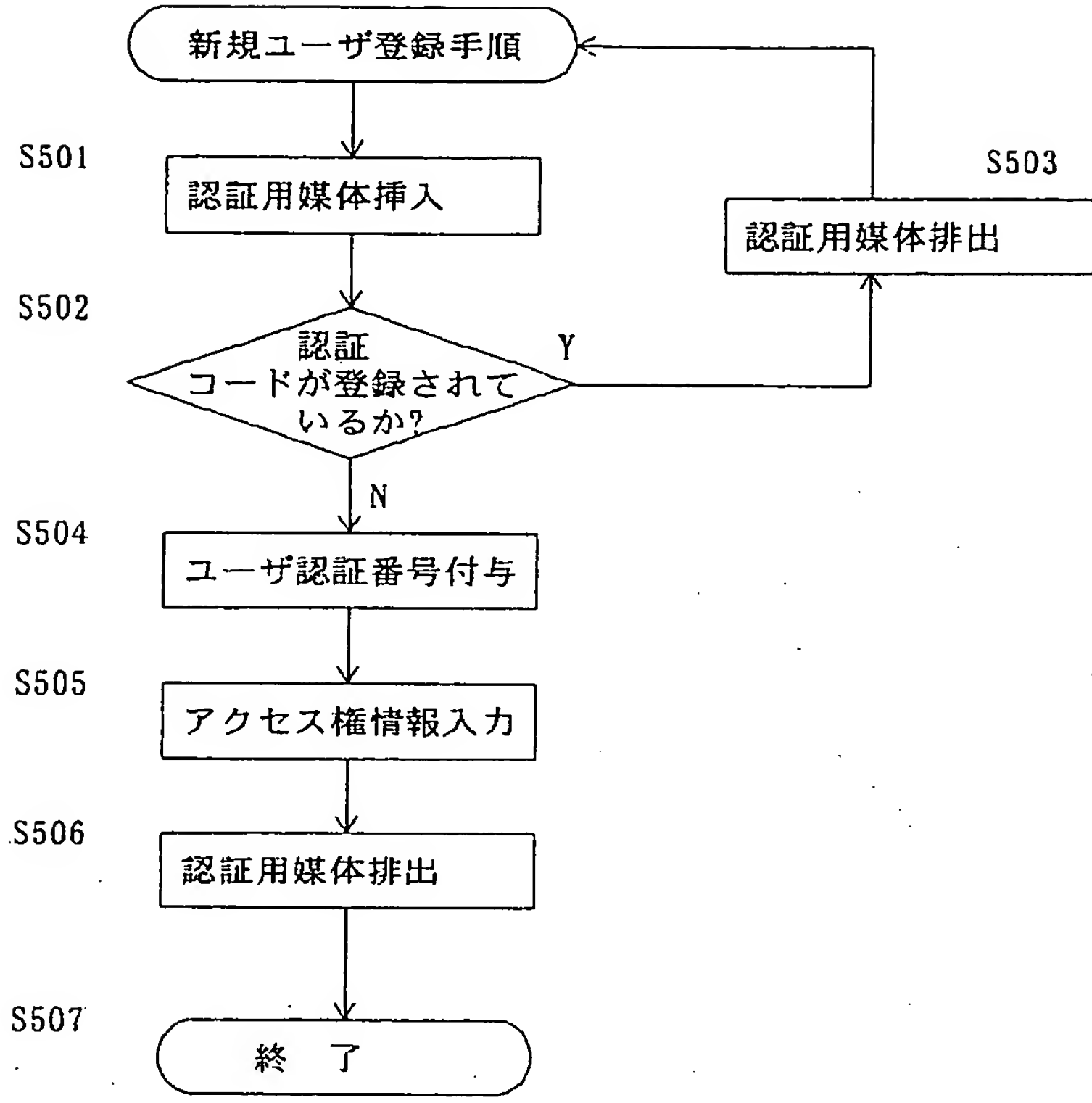
(14)

【図8】



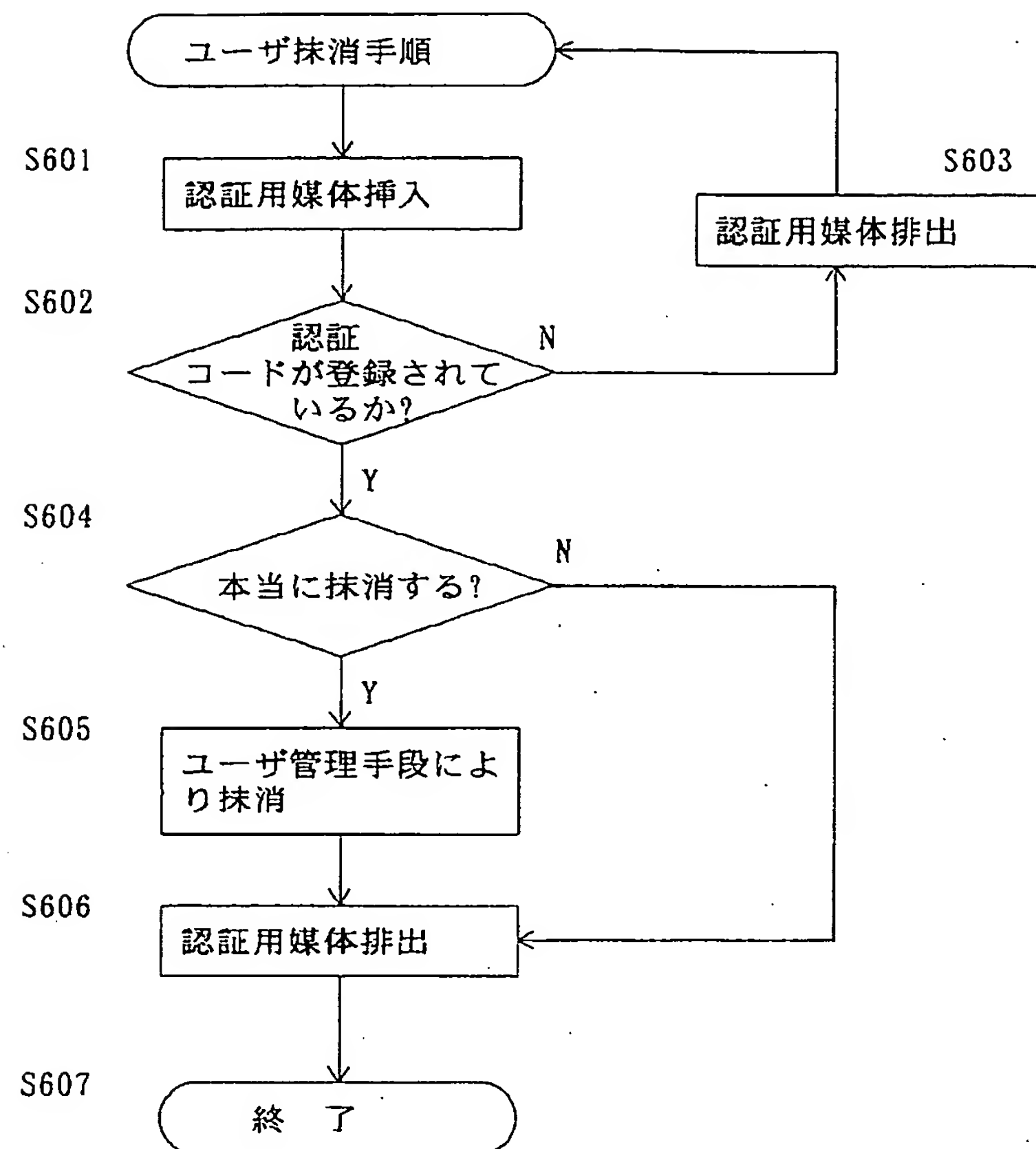
(15)

【図9】



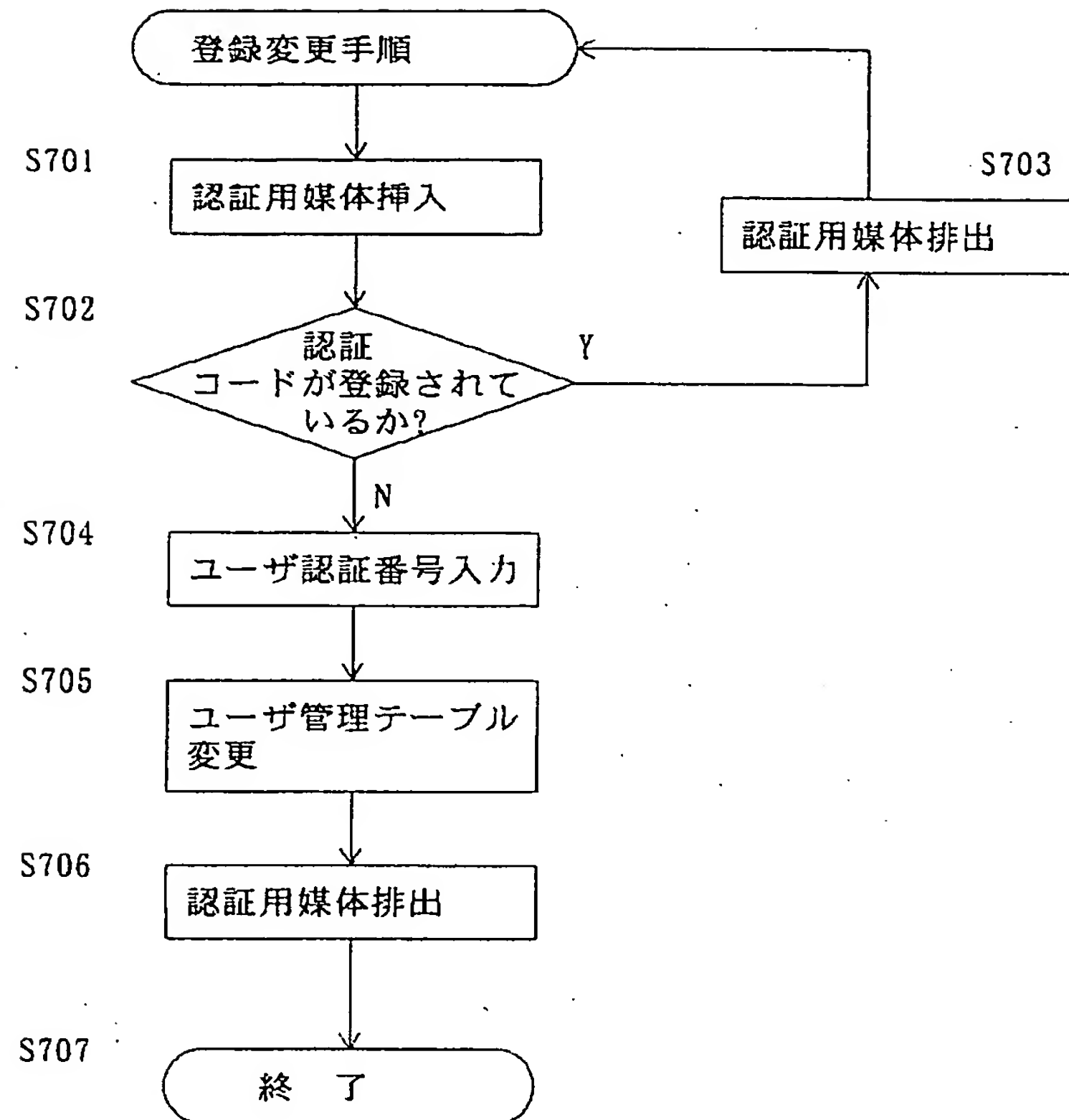
(16)

【図10】



(17)

【図11】



フロントページの続き

(72)発明者 岡田 雄治
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 高橋 直樹
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 久富 健治
大阪府門真市大字門真1006番地 松下電器
産業株式会社内